

(51)Int.Cl.⁵

識別記号

庁内整理番号

FI

技術表示箇所

H 0 4 L 9/06

9/14

G 0 9 C 1/00

8837-5L

H 0 4 B 7/26

1 0 9 R

7304-5K

7117-5K

H 0 4 L 9/ 02

Z

審査請求 有 請求項の数24(全 14 頁)

(21)出願番号 特願平4-267808

(22)出願日 平成4年(1992)9月11日

(31)優先権主張番号 ~~785103109~~

(32)優先日 1991年9月13日

(33)優先権主張国 米国(US)

(71)出願人 390035493

アメリカン テレフォン アンド テレグ
ラフ カムパニーAMERICAN TELEPHONE
AND TELEGRAPH COMPA
NYアメリカ合衆国 10013-2412 ニューヨ
ーク ニューヨーク アヴェニュー オブ
ジ アメリカズ 32

(74)代理人 弁理士 三俣 弘文

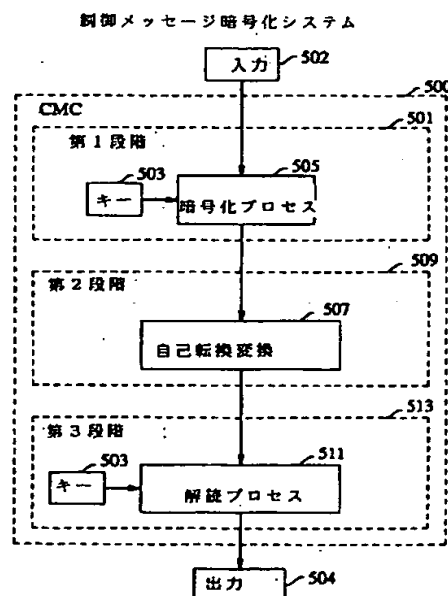
最終頁に続く

(54)【発明の名称】 暗号化システム

(57)【要約】

【目的】 セルラー電話システムにおける暗号システムにおいて、可変長の元メッセージを、8ビットマイクロコンピュータによって簡単に暗号化及び解読を行うことが可能な、比較的安全な、自己転換、対称キー暗号システムを提供することを目的とする。

【構成】 8ビットマイクロコンピュータで効率よく実効可能な、比較的安全で、自己転換、対称キー暗号システムによるキー暗号システムに関する。本暗号システムは、セルラー電話への応用に特に適している。本暗号システムは、3つの段階から構成される：1)自動キー暗号化、2)第1段階で暗号化されたメッセージの一部から導出されたキーを用いた、1回限り暗号通信法の利用、3)第1とは逆の第2の自動キー解読からなる。



【特許請求の範囲】

【請求項1】 通信システムにおいて、メッセージを表すメッセージ信号の集合を変換する方法において、第1の中間信号の集合を形成するために、暗号化プロセス(505)およびキー信号の集合(503)によって前記メッセージ信号の集合を暗号化するステップと、第2の中間信号の集合を形成するために、インボリュート変換(507)に従って前記第1中間信号の集合を変更するステップと、

出力信号の集合を形成するために、前記暗号化プロセスの逆である解読プロセス(511)によって、前記第2中間信号の集合を解読するステップとを有し、前記変更ステップが、前記第1中間信号の集合の第1の部分集合に基づいた非キー変換によって、前記第1の中間信号の集合の第2の部分集合を修正するステップからなることを特徴とする暗号化方法。

【請求項2】 前記暗号化ステップが、第1の自動キープロセスに従った、前記第1の中間信号を形成するステップを有し、前記解読ステップが、第2の自動キープロセスに従った、前記出力信号を形成するステップを有することを特徴とする、請求項1に記載の暗号化方法。

【請求項3】 ソース信号の集合から、前記キー信号の集合を導出するステップを有することを特徴とする、請求項1に記載の暗号化方法。

【請求項4】 前記導出ステップが、前記キー信号の集合を形成するために、前記ソース信号の集合とともに、パターン信号の集合をハッシュするステップからなることを特徴とする、請求項3に記載の暗号化方法。

【請求項5】 前記キー信号の集合および前記パターン信号の集合が、 N を正の整数として、 N 個の要素をそれぞれ有することを特徴とする、請求項4に記載の暗号化方法。

【請求項6】 前記導出ステップが、前記ハッシュステップで用いることのできる、前記パターン信号の集合を作成するステップを有することを特徴とする、請求項5に記載の暗号化方法。

【請求項7】 N および D を正の整数として、前記キー信号の集合が N 個の要素を有し、メッセージ信号の集合が D 個の要素を有することを特徴とする、請求項1に記載の暗号化方法。

【請求項8】 前記メッセージ信号の集合を暗号化する場合、前記ステップが、信号 z を選択された大きさに設定するステップと、 $0 \leq i < D$ の範囲の相異なる整数値信号 i に対し、前記信号 i および z の各大きさに基づいて信号 q を設定するステップと、信号 k を、前記信号 q および $T[q]$ (ただし $T[q]$ は前記キー信号の集合の q 番目の要素)の各大きさに基づいて設定するステップと、前記第1の中間信号の集合の i 番目の要素を、前記メッ

セージ信号の集合の前記第 i 要素および前記信号 k の各大きさに基づいて生成するステップと、前記信号 z の大きさを、前記第1の中間信号の集合の第 i 要素および前記信号 z の各大きさに基づいて更新するステップとからなることを特徴とする、請求項7に記載の暗号化方法。

【請求項9】 前記メッセージ信号の集合を暗号化する場合、前記ステップが、

n ビット信号 z を選択された大きさに設定するステップと、

$0 \leq i < D$ の範囲の連続する整数値をとるインデックス i に対し、

n ビット信号 q を $z \# m$ に(ただし、 $\#$ はビットごとのブール排他的OR演算子であり、 m は $i \bmod 2^n$)設定するステップと、

n ビット信号 k を $T[q]$ に(ただし $T[q]$ は前記キー信号の集合の n ビット要素)設定するステップと、

前記メッセージ信号の集合の前記 i 番目の n ビット要素と n ビット信号 k を、 2^n を法として加算することによって、前記第1の中間信号の集合の i 番目の n ビット要素を生成するステップと、

前記第1の中間信号の集合の前記 i 番目の n ビット要素と n ビット信号 z を、 2^n を法として加算することによって、前記 n ビット信号 z の大きさを更新するステップとからなることを特徴とする、請求項7に記載の暗号化方法。

【請求項10】 前記各 n ビットが8ビットであり、 2^n が256に等しいことを特徴とする、請求項9に記載の暗号化方法。

【請求項11】 前記第1の中間信号の前記変更ステップが、 $0 \leq i < (D-1)/2$ の範囲で、 $b(i) \# q$ に等しい前記第2の中間信号の集合の i 番目の要素を生成する(ただし、 $b(i)$ は前記第1の中間信号の集合の i 番目の要素、 q は $b(x)$ に基づき、 x は D および i の値に基づき、 $b(x)$ は前記第1の中間信号の集合の x 番目の要素で、 $\#$ はビットごとのブール排他的OR演算子)ステップからなることを特徴とする、請求項7に記載の暗号化方法。

【請求項12】 前記第2の中間信号の集合を解読する場合、前記ステップが、

信号 z を選択された大きさに設定するステップと、

$0 \leq i < D$ の範囲の相異なる整数値信号 i に対し、

前記信号 i および z の各大きさに基づいて信号 q を設定するステップと、

信号 k を、前記信号 q および $T[q]$ (ただし、 $T[q]$ は前記キー信号の集合の q 番目の要素)の各大きさに基づいて設定するステップと、

前記 z 信号の大きさを、前記第2の中間信号の集合の第 i 要素および前記信号 z の各大きさに基づいて更新するステップと、

前記出力信号の集合の i 番目の要素を、前記第2の中間信号の集合の前記第 i 要素および前記信号 k の各大きさに基づいて生成するステップとからなることを特徴とする、請求項7に記載の暗号化方法。

【請求項13】 前記第2の中間信号の集合を解読する前記ステップが、

n ビット信号 z を選択された大きさに設定するステップと、

$0 \leq i < D$ の範囲の連続する整数値をとるインデックス i に対し、

n ビット信号 q を $z \# m$ に (ただし、 $\#$ はビットごとのブール排他的OR演算子であり、 m は $i \bmod 2^n$) 設定するステップと、

n ビット信号 k を $T[q]$ に (ただし、 $T[q]$ は前記キー信号の集合の前記 q 番目の n ビット要素) 設定するステップと、

前記第2の中間信号の集合の前記 i 番目の n ビット要素と前記信号 z を、 2^n を法として加算することによって、前記 n ビット信号 z の大きさを更新するステップと、

前記第2の中間信号の集合の i 番目の要素から n ビット信号 k を、 2^n を法として減算することによって、前記出力信号の集合の i 番目の n ビット要素を生成するステップとからなることを特徴とする、請求項7に記載の暗号化方法。

【請求項14】 前記各 n ビットが、8ビットで、 2^n が256に等しいことを特徴とする、請求項12に記載の暗号化方法。

【請求項15】 前記メッセージ信号の集合が、セルラ電話システムにおけるメッセージを表すことを特徴とする、請求項1に記載の暗号化方法。

【請求項16】 前記メッセージ信号の集合が、音声を表すことを特徴とする、請求項1に記載の暗号化方法。

【請求項17】 前記メッセージ信号の集合が、非音声データを表すことを特徴とする、請求項1に記載の暗号化方法。

【請求項18】 前記メッセージ信号の集合が、無線通信システムにおけるメッセージを表すことを特徴とする、請求項1に記載の暗号化方法。

【請求項19】 メッセージを表すメッセージ信号の集合を変換するための暗号化システムにおいて、第1の中間信号の集合を形成するために、暗号化プロセスおよびキー信号の集合(503)によって前記メッセージ信号の集合を暗号化する手段(210)と、第2の中間信号の集合を形成するために、インボリュート変換によって前記第1の中間信号の集合を変更する手段(210)と、

出力信号の集合を形成するために、前記暗号化プロセスの逆である解読プロセスによって前記第2の中間信号を解読する手段(210)とを有し、

前記変更手段が、前記第1中間信号の集合の第1の部分集合に基づいた非キー変換によって、前記第1の中間信号の集合の第2の部分集合を修正する手段からなることを特徴とする暗号化システム。

【請求項20】 前記暗号化手段が、第1の自動キープロセスに従って前記第1の中間信号の集合を形成する手段からなり、前記解読手段が、第2の自動キープロセスに従って前記出力信号の集合を形成する手段からなることを特徴とする、請求項19に記載の暗号化システム。

10 【請求項21】 N および D を正の整数として、前記キー信号の集合が N 個の要素を有し、メッセージ信号の集合が D 個の要素を有することを特徴とする、請求項19に記載の暗号化システム。

【請求項22】 前記メッセージ信号の集合を暗号化する前記手段が、

信号 z を選択された大きさに設定する手段と、

$0 \leq i < D$ の範囲の相異なる整数値に信号 i を設定する手段と、

20 前記信号 i および z の各大きさに基づいて信号 q を設定する手段と、

信号 k を、前記信号 q および $K[q]$ (ただし、 K

$[q]$ は前記キー信号の集合の q 番目の要素) の各大きさに基づいて設定する手段と、

前記第1の中間信号の集合の i 番目の要素を、前記メッセージ信号の集合の前記第 i 要素および前記信号 k の各大きさに基づいて生成する手段と、

30 前記信号 z の大きさを、前記第1の中間信号の集合の第 i 要素および前記信号 z の各大きさに基づいて更新する手段とからなることを特徴とする、請求項21に記載の暗号化システム。

【請求項23】 前記第1の中間信号の集合の前記変更手段が、 $0 \leq i < (D-1)/2$ の範囲で、 $b(i) \# q$ に等しい前記第2の中間信号の集合の i 番目の要素

(ただし、 $b(i)$ は前記第1の中間信号の集合の i 番目の要素であり、 q は $b(x)$ に基づき、 x は D および i の値に基づき、 $b(x)$ は前記第1の中間信号の集合の x 番目の要素であり、 $\#$ はビットごとのブール排他的OR演算子) を生成することを特徴とする、請求項21に記載の暗号化システム。

40 【請求項24】 前記第2の中間信号の集合を解読する前記手段が、

信号 z を選択された大きさに設定する手段と、

$0 \leq i < D$ の範囲の相異なる整数に信号 i を設定する手段と、

前記信号 i および z の各大きさに基づいて信号 q を設定する手段と、

信号 k を、前記信号 q および $K[q]$ (ただし、 K

$[q]$ は前記キー信号の集合の q 番目の要素) の各大きさに基づいて設定する手段と、

50 前記信号 z の大きさを、前記第2の中間信号の集合の第

i 要素および前記信号 z の各大きさに基づいて更新する手段と、

前記出力信号の集合の i 番目の要素を、前記第 2 の中間信号の集合の前記第 i 要素および前記信号 k の各大きさに基づいて生成する手段とからなることを特徴とする、請求項 21 に記載の暗号化システム。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、暗号化方法に関し、セルラ電話における通信のプライバシー確保のための暗号システムに関する。

【0002】

【従来の技術】従来の電話においては、各電話セット（ファックス、モデム等）は、ローカルセントラルオフィスの交換機の 1 つのポートに、物理的に接続される。接続は、与えられた電話線あるいは電話線の指定のチャネルを介して行われる。電話線の接続はサービス提供者（通常は通信事業者）によって行われ、従ってサービス提供者は、チャネルの通話が加入者によるものであることを確信できる。一方、無線電話での加入者の認証は不確かなものである。

【0003】米国における現在のセルラ電話構成では、加入者が呼び出しを行うと、課金のためそのセルラ電話がサービス提供者に発信者の身元を通知する。この情報は暗号化されていない。第 3 者がその時点で盗聴すると、加入者の身元情報が得られてしまう。この情報には、加入者の電話番号、加入者の装置の電気シリアル番号（ESN）が含まれている。従って、盗聴者はそのセルラ電話をプログラムして正式な加入者になりすまし、サービスを受けることが可能となる。あるいは、通話中に割り込んで、送信電力を増加させることによって、サービス提供者にある制御コードを送って接続に侵入することもできる。サービス提供者は、接続時および／あるいは通話中の発信者の身元の確認機構を持たないため、このような侵害は基本的に避けられない。

【0004】盗聴者が身元情報を知ろうとすれば、割当てセル内の全セルラ周波数帯を、自動的に掃引する装置を用いることができる。従って、セルラ電話サービスの侵害を阻止できない。また、音声信号を暗号化していないため、会話の内容を盗聴することができる。つまり、セルラ電話システムにおいて効果的な保護手段が必要とされており、利用者の認証およびプライバシー保護のために、暗号化の利用が必要とされる。

【0005】

【発明が解決しようとする課題】いくつかの標準的な暗号方法は、セルラ電話等の一般的な認証問題の解決に用いることができるが、実際上の問題もある。まず、プライベートキー暗号アルゴリズムに基づいた、従来の要求／応答プロトコルを用いることができる。この方法では、加入者の移動ステーションに秘密キーが割り当てら

れ、このキーはホームシステムにも登録されている。提供システムが加入者を認証する場合には、ホームシステムに対して、その加入者の利用に関して照会を行う。ホームシステムは不定期に要求を行い、加入者からのキーを伴う要求に対して、対応する応答を行う機能を果たす。要求および応答は提供システムによって行われ、移動ステーションへの要求も行う。移動ステーションは、要求とその記憶された秘密キーとを処理した結果を応答する。提供システムは、ホームステーションおよび移動ステーションからの応答を比較し、一致した場合に認証されたと見なす。

【0006】この方法の問題点は、提供システムが発信時の認証の際に、十分早くホームシステムに接続することができず、ホームシステムのデータベースソフトウェアが加入者の秘密キーを調べ、要求／応答ペアを構成することを短期間に行うことができない点である。ネットワークあるいはソフトウェアの数秒の遅延は、加入者が発信する際に、受話器を持ち上げてからダイヤルトーンが聞こえるまでのデッドタイムを増し、さらに（セルラ提供者の現在用いている制御ネットワークおよび交換装置によって）遅延時間が増す。現状では、そのような遅延は許容されない。

【0007】パブリックキー暗号システムは、認証問題を解決するもう一つの標準的な方法である。一般的に、各移動ステーションはサービス提供者のパブリックキーによって、“パブリックキー証書”が与えられ、その移動ステーションがサービス提供者の合法的な利用者であることを示す。さらに、各移動局に秘密データ（プライベートキー）が与えられ、証書と同時に第 3 者に合法的な利用者であることを示すのに用いられる。

【0008】例として、サービス提供者は RSA キーペア（F, G）を、F をプライベート、G をパブリックとして有する。サービス提供者は各移動局に、その RSA キーの独自のペア（D, E）を、F（E）（提供者のプライベートキー F を用いて移動局のパブリックキー E を暗号化したもの）と共に与える。移動局は、提供システムに、（E, F（E））を送ることによってその身元を提示する。提供システムでは、F（E）に G を用いて E を得る。提供システムは要求 X を生成し、移動局のパブリックキー E を用いて暗号化して E（X）を得て、それを移動局へ送る。移動局は、E（X）にプライベートキー D を用いて X を得て、解読した状態でそれを応答として提供システムへ返送する。

【0009】この問題について、処理あるいはデータ伝送量を減少させる改良例もあるが、セルラ電話で現在用いられているハードウェアにおいて、数秒以下で効率的に実行できる、パブリックキー認証方法は存在しない。認証時には、提供システムとホームシステム間でのネットワークの接続性は必要とされないが、従来方法での時間的な制限が問題となるように、パブリックキー方法で

も同様の制約が生じる。

【0010】

【課題を解決するための手段】本発明では、可変長の元メッセージを、8ビットマイクロコンピュータによって簡単に暗号化および解読を行うことが可能である。本発明は、比較的安全な、自己転換、対称キー暗号システムで、3段階から構成される。第1段階は、元テキストの自動キー暗号化である。第2段階は、自己転換暗号化で、暗号キーは第1段階で暗号化されたメッセージの一部から導出される。第3段階は、第2の自動キー解読で、第1段階の自動キー暗号化に対応する。

【0011】

【実施例】移動セルラ電話システムでは、多数の移動電話、少数のセルラ無線提供者（各提供者が複数の基地局を有する）、複数の交換ネットワーク提供者（通信事業者）から構成される。セルラ無線提供者と通信事業者は、セルラ電話加入者によって、セルラおよび非セルラ両者の電話加入者との通話を可能にするように組合せられる。図1に概略の構成を示すように、通信事業者IおよびIIは、交換機10-14を有する交換ネットワークを形成して結合される。固定局ユニット20および21は交換機10に接続され、移動局ユニット22および23は不特定位置で、基地局30-40は交換機10-14に接続される。基地局30-34は提供者1、基地局35および36は提供者2、基地局37は提供者4、基地局38-40は提供者3にそれぞれ属する。本発明の目的では、基地局は複数の送信器を有するセルと同じ意味である。セルの集合体は、図1の基地局30、31および32のように、地理上のセルラサービスエリア（CGSA）を形成する。

【0012】各移動局ユニットは、そのユニット固有の電気シリアル番号（ESN）を有する。ESN番号はユニットの製造時に、製造者によって割り当てられ（例えば、ROM内に）、アクセスはできるが変更はできない。

【0013】利用者がその移動電話ユニットのサービスアカウントを申請すると、サービス提供者は利用者に、電話番号（MIN1呼称）、エリアコード（MIN2呼称）、“秘密キー”（Aキー）を割り当てる。MIN1およびMIN2呼称は提供者のCGSAに関連し、図1の構成の全基地局は、特定のMIN2およびMIN1ペアの属するCGSAを識別することができる。Aキーは、利用者装置および提供者のCGSAプロセッサ（図1には示さず）だけが知っている。CGSAプロセッサは、ユニットのESN、Aキー、MIN1およびMIN2呼称の他、サービス提供者の必要な情報を保持している。

【0014】MIN1呼称およびAキーがインストールされ、CGSAプロセッサが、移動局ユニットに特定のランダムシーケンス（RANDSSD）を送信し、“共

有秘密データ”（SSD）の作成を指示することによって、利用者のユニットが初期化される。（CGSAは、RANDSSDおよびSSDフィールドの生成を、移動局ユニットの存在するセルの基地局を通して送信する。）SSDフィールドの作成は図2に示されるプロトコルに従う。

【0015】図1の構成では、各基地局は、あらかじめ割り当てられたチャネルのいくつかを用いて、そのセル内の全てのユニットに情報を送信する（送信バンド）。さらに、各移動局ユニットに対して、相互に確認した、（一時的に）割り当てられたチャネルによって、双方向通信を確保する。基地局と移動局ユニットで、通信チャネルの確認を行う方法は、本発明には重要でないため、ここでは詳しく述べない。例としては、移動局ユニットが全チャネルをスキャンし開きチャネルを選択する方法が考えられる。その後基地局へ、そのMIN2およびMIN1呼称を送信し（元テキストあるいはパブリックキーによって暗号化されたもののいずれか）、基地局に認証プロセスの開始を許可する。認証通信が確立されると、基地局は移動局を他のチャネルへスイッチしても良い。

【0016】本発明による移動電話システムでの呼び出しの確立と保持方法では、認証プロセスは会話中に多数回行われる。従って、認証プロセスは比較的安全で簡単に行うことができる。設計を簡単にし導入費用を抑えるために、移動局ユニットおよび基地局の両方で同じプロセスを用いるべきである。

【0017】多くの認証プロセスは、プロセスを行うために、ハッシング機能あるいは一方機能を用いる。ハッシング機能は、“秘密キー”をサインに変換する、多対一のマッピングを実行する。以下に、簡単で、速く、効果的で、柔軟性のあるハッシング機能の一例を示す。これは、本発明の認証プロセスに好都合であるが、他のハッシング機能を用いることもできる。

【0018】ジャンブルプロセス

ジャンブルプロセスでは、dの“秘密”データワードb(i)の“サイン”を、kワードのキーx(j)によって生成する。ここで、d、i、j、およびkは整数である。“サイン”の生成プロセスは、1回に一つのデータワードを実行する。この説明のために、ジャンブルプロセスで操作するワードが8ビット長（0から256の範囲）であるとするが、他のワードサイズでも実行できる。“秘密”データブロック長を、鋸歯状波関数に用いて、

$$s_d(t) = t \quad 0 \leq t \leq d-1$$

$$s_d(t) = 2d-2-t \quad d \leq t \leq 2d-3$$

$$s_d(t) = s_d(t+2d-2) \quad (\text{全}t\text{に対して})$$

とする。この関数は、z=0およびi=0から始め、 $0 \leq 6d-5$ の範囲で連続的に増加する整数iに対する以下のプロセスで用いられ、a) b(s_d(i))を、b

$(s_d(i)) \cdot b(s_d(i)) + x(i_k) + SBOX(z) \bmod 256$ によって更新し、ここで、 i_k は $i \bmod k$ 、 $SBOX(z) = y + [y/2048] \bmod 256$ 、 $y = (z \# 16) \cdot (z + 1) \cdot (z)$ とし、 $[y/2048]$ は y を2048で割った整数部を示し、 $\#$ はビット排他OR関数である； $b) z$ を、 $z = z + b(s_d(i)) \bmod 256$ によって更新する。

【0019】上記のプロセスでは、データとキーの間に明確な区別は無いことが分かる。従って、認証に用いられるどの符号列も、上記のプロセスでキーとして用いられる部分を有することができる。逆に、キーと結合されたデータワードは、“認証”符号列と考えられる。各ワード $b(i)$ は、 $0 \leq i < d-1$ で1回に一つそれぞれ分割され、ハッシングを“適切”に行うことができる。ハッシングプロセス自体には、余分のバッファは必要とされない。

【0020】上述のプロセスで必要とされる操作は、シフト(2048による割り算)、切捨て(□関数および $\bmod 256$ 関数)、加算、乗算、およびビット排他OR関数であるため、基本的な従来のプロセッサで簡単に実行できる。

【0021】図2のSSDフィールドの初期プロセスに戻って、RANDSSDシーケンスおよび新規のSSDフィールド(図2の矢印)の作成指示が移動ステーションで受信されると、図3に従って新規のSSDフィールドが生成される。移動局ユニットは、ESN呼称、Aキー、RANDSSDシーケンスを結合して認証符号列を形成する。認証符号列はジャンブルブロック101(前述)へ導かれ、SSDフィールドを出力する。SSDフィールドは2つのサブフィールドから構成される：認証手順の補助に用いられるSSD-Aサブフィールド、および音声プライバシー手順およびある信号メッセージ(後述)の暗号化を補助に用いられるSSD-Bサブフィールドである。多数のSSDサブフィールドが生成される。全ビット数を多くする必要がある場合には、データビット数の多いものから始めればよい。以下に述べるように、これは通常必要とされることはない。

【0022】ホームCGSAプロセッサは、受信されたMIN2およびMIN1呼称の割り当てられた移動局ユニットのESNおよびAキーを知っている。また、送信したRANDSSDシーケンスも知っている。従って、ホームCGSAプロセッサでは、移動局ユニットのSSDフィールド生成プロセスを複製する。RANDSSD信号を、ESN呼称およびAキー、前述のジャンブルプロセスと結合することによって、CGSAプロセッサは新規のSSDフィールドを生成し、それをSSD-AおよびSSD-Bのサブフィールドに分割する。しかし、ホームプロセッサで生成されたSSDフィールドは検証されねばならない。

【0023】図2のように、SSDフィールドの検証は移動局ユニットによって行われる。移動局ユニットはブロック102においてランダム要求シーケンス(RANDBSシーケンス)を生成し、サーバ基地局を通じてホームCGSAプロセッサへそれを送信する。図4のように、ホームCGSAプロセッサは、要求RANDBSシーケンス、移動局ユニットのESN、MIN1呼称、新規生成されたSSD-Aを結合し、ジャンブルプロセスで用いられる認証符号列を形成する。この例では、ジャンブルプロセスは、移動局へ送られる分割された認証信号AUTHBSを生成する。移動局はまた、RANDBSシーケンス、ESN呼称、MIN1呼称、新規生成されたSSD-Aを結合し、ジャンブルプロセスで用いられる認証符号列を形成する。移動局は、そのジャンブルプロセスの結果と、ホームCGSAプロセッサからの分割された認証信号(AUTHBS)とを比較する。比較ステップ(ブロック104)で一致すると、移動局は、SSDフィールドの更新に成功したことを示す確認メッセージを、ホームCGSAプロセッサへ送る。一致しない場合には、その比較結果を移動局が送信する。

【0024】移動局が初期化されても、SSDフィールドは、ホームCGSAプロセッサが新規のSSDフィールドを生成することを指示するまで、そのまま保持される。これは例えば、SSDフィールドが処理されたことが認められる場合に生じる。そのような場合、ホームCGSAプロセッサは移動局にもう一つのRANDSSDシーケンスを送り、新規のSSDフィールドを生成するように指示する。

【0025】前述のように、セルラ電話では各基地局から、そのセル内の全ての移動局ユニットのために、種々の情報信号が送信される。図1の構成では、基地局から送信される信号の一つは、ランダムあるいは疑似ランダムシーケンス(RANDシーケンス)である。RANDシーケンスは、移動局ユニットで生成および送信された信号をランダム化して、種々の認証プロセスに用いられる。RANDシーケンスは、録音/再生による妨害を防ぐために定期的に変更されねばならない。RAND信号の待ち時間の設定方法として、予想される平均呼び出し時間より短く設定する方法がある。従って、通常移動局では、連続する呼び出しに対して異なったRAND信号を用いることになる。

【0026】本発明では、移動局ユニットがセルに入るとすぐに、認証されるように基地局ユニットに登録し、移動局からの呼び出しと、基地局からの移動局への呼び出しが行えるようにする。移動局がサーバ基地局に登録されると、サーバ基地局へ、MIN1およびMIN2呼称およびESNシーケンスを送信する。認証プロセスは登録の際に行われ、そのプロセスを図5に示す。図5のように、移動局はRANDシーケンスを受信し；ESNシーケンス、MIN1呼称、SSD-Aサブフィールド

を結合し、ジャンブルプロセスで用いられる認証符号列を形成する。ジャンブルプロセスの出力の、分割された認証符号列は、ESNシーケンスと共にサーバ基地局へ送られる。

【0027】ある実施例では、分割された認証符号列が基地局へ届くまでにRANDシーケンスが変化する可能性があるため、移動局ユニットで用いられるRANDシーケンスの全部あるいは一部もまたサーバ基地局へ送られる。

【0028】サーバ基地局は、RANDシーケンスを生成したためそれを知っている。基地局はまた、移動局ユニットを識別するための、ESN、MIN2およびMIN1呼称をも知っている。しかし、最初の登録時には、サーバ基地局は移動局ユニットのSSDフィールドを知らない。しかし、移動局ユニットのホームCGSAプロセッサを知っている(MIN1およびMIN2呼称から)ため、認証プロセスは以下になる。サーバ基地局は、ホームCGSAプロセッサに、MIN1呼称、ESNシーケンス、移動局ユニットが送信した分割された認証符号列、分割された認証符号列を生成するために移動局ユニットが用いたRANDシーケンスを送信する。移動局ユニットのMIN1呼称およびESNシーケンスから、ホームCGSAプロセッサは、移動局ユニットのSSD-Aサブフィールドを知り、前述のように認証符号列を生成し、ジャンブルプロセスへ導く。ホームCGSAプロセッサによって生成された分割された認証符号列が、移動局ユニットによって生成され、サーバ基地局から送られた分割された認証符号列と一致する場合

には、検証は成功したと見なされる。この場合、ホームCGSAプロセッサは、サーバ基地局にユニットのSSDフィールドを与える。ESN呼称およびSSDフィールドの安全を確保するために、基地局とCGSAプロセッサ間の通信は暗号形式で行われる。

【0029】移動局ユニットが(前述のプロセスによって)サーバ基地局で認証されると、サーバ基地局は移動局ユニットのESNおよびSSDフィールドを所有し、そのセル内のその後の認証プロセスはサーバ基地局内で、ホームCGSAプロセッサを参照することなく進めることができる。SSDフィールドを更新する際には、ホームCGSAプロセッサおよび移動局ユニット間で通信し、基地局はそれらの間を取り持つだけとなる。つまり、ホームCGSAプロセッサは、RANDSSDシーケンスを生成し、RANDSSDシーケンスに基づいてSSDフィールドを更新し、サーバ基地局にRANDSSDシーケンスおよび新規に生成されたSSDフィールドを与え、サーバ基地局は、移動局ユニットに、そのSSDフィールドを更新しサーバ基地局に要求を送るように指示し、AUTHBS符号列(前述)を生成し、それを移動局ユニットへ送り、移動局ユニットはAUTHBS符号列を検証し、サーバ基地局へ、移動局ユニットお

よびサーバ基地局が同じSSDフィールドを有することを通知する。

【0030】図6に示すように、サーバ基地局によって登録されると、移動局ユニットは発信することができる。発信シーケンスでは、RAND、ESN、SSD-A信号、受信者を識別する(電話)番号を結合する。結合された信号は、サーバ基地局で検証できる、分割された認証シーケンスのために、ジャンブルプロセスへ送られる。基地局で検証できるように、受信者の識別番号(および前述のRAND信号の一部)は基地局で受信できるような状態、つまり元テキストでも送信されねばならない。認証シーケンスが検証されると、基地局は発信を処理し、受信者との接続を行う。

【0031】移動局ユニットが“受信者”である場合の接続プロトコルは、図5の登録プロトコルに従う。つまり、サーバ基地局が呼び出された移動局に、RANDシーケンス、ESN呼称、MIN1呼称およびSSD-Aサブフィールドから生成された認証シーケンスを送信するように要求する。認証されると、基地局と受信者の移動局ユニット間に経路が設定され、発信した移動局(あるいは固定局)とのデータのやり取りを行えるようにする。

【0032】上記の認証は(検証されることを考慮して)、認証されたパケットあるいは符号列それ自身に関してのみ有効である。それ以外に安全性を高めるには、3つの異なった追加保護手段が用いられる。これらは、音声暗号化、不定期の再認証、制御メッセージの暗号化である。

【0033】音声暗号化

音声信号は第1に、デジタル形式にすることで暗号化される。これは、圧縮の有無、誤り訂正コードの有無を問わず種々の従来方法で行うことができる。デジタル信号のビットはKビット毎のグループに分割され、各グループが暗号化される。移動局ユニットおよび基地局において、RANDシーケンス、ESNおよびMIN1呼称、SSD-Bサブフィールドが結合され、ジャンブルプロセスへ導かれる。ジャンブルプロセスでは2Kビットが作られ、Kビット毎のグループAおよびBに分けられる。移動局ユニットのグループAは出力音声の暗号化に用いられ、グループBは入力音声の解読に用いられる。一方、基地局ではグループAは入力音声の解読に用いられ、グループBは出力音声の暗号化に用いられる。図7に音声の暗号化および解読プロセスを示す。

【0034】再認証

基地局では、再認証プロセスによって、基地局が動作を検知した移動局ユニットが、本当に動作を認可された移動局ユニットであるかを確認する。これは、図8に示されるように、基地局が移動局ユニットに、分割された認証シーケンスを送信するように要求すれば良い。そのような各要求に対して、基地局は特別(RANDU)シー

ケンスを送信する。移動局ユニットは、RANDUシーケンス、移動局ユニットのエリアコードMIN2呼称、ESN呼称、MIN1呼称、SSD-A呼称を結合して、分割された認証シーケンスを生成する。結合された符号列は、ジャンブルプロセスへ導かれ、その結果得られた、分割された認証符号列が基地局へ送信される。この地点で基地局は、分割された認証符号列が有効であるかどうかを検証する。

【0035】制御メッセージ暗号システム

第3の安全方法では、制御メッセージを保護する。通話中には、種々の状況において、制御メッセージを伝える必要がある。ある場合には、制御メッセージは、発信した移動局あるいは基地局のどちらかに重大な悪影響を及ぼす可能性がある。そのため、通話中に送られるある種の制御メッセージは（十分に）暗号化されていることが望ましい。あるいは、ある種のメッセージ形式のあるフィールドを暗号化しても良い。これには、クレジットカード番号のような“データ”制御メッセージおよび発信再定義制御メッセージが含まれる。これは、制御メッセージ暗号システムによって行われる。

【0036】制御メッセージ暗号システム（CMC）は対称キー暗号システムで、以下の特徴を有する：

1) 比較的安全、2) 8ビットコンピュータで効率良く動作する、3) 自己転換である（すなわちインボリュート）。

【0037】CMCの暗号キーは、256バイトの配列TBOX[z]で、“秘密キー”（例SSD-Bサブフィールド）から以下のように導かれる： $0 \leq z < 256$ の範囲の各zに対して、 $TBOX[z] = z$ と設定し、配列TBOX[z]および秘密キー（SSD-B）をジャンブルプロセスへ導く。これは本質的に、図7の要素301、302および303に示されるものである（ただし、図7のバイト数は256ではなく2Kである）。

【0038】キーが導かれると、CMCは制御メッセージの暗号化および解読に用いることができる。あるいは、キーの用いられる各時間に、“素早く”キーを導くことも可能である。CMCは複数バイトの可変長メッセージの暗号化を行うことができる。CMCの動作は、自己転換で、相互的あるいはインボリュートである。つまり、元テキストを暗号化されたテキストから得るための操作と、元テキストを暗号化したテキストを得るための操作とは完全に同じである。インボリュート関数は、それ自身の逆関数である（例、 $x = 1/x'$ 、 $x = T(T(x'))$ ）。従って、CMC操作を2回行っても、バッファの内容は変化しない。

【0039】以下の説明では、暗号化プロセス（解読プロセス）では、元のテキスト（暗号化されたテキスト）がデータバッファ内に保持され、CMCはデータバッファ内の内容を操作して、データバッファの内容が最終的に暗号化されたテキスト（あるいは解読されたテキス

ト）を構成することを仮定する。これは、図9の要素502および504が一つの同じレジスタで良いことを示す。

【0040】CMCは連続する3つの段階から構成され、それぞれデータバッファ内の各バイト符号列を更新する。全体としてのCMCおよびCMCの第2段階はインボリュートである。データバッファがdバイトで、iを $0 \leq i < d$ の範囲として、各バイトをb(i)で表す：CMCの第1段階は以下になる：zの初期値を0とし、iを $0 \leq i < d$ の範囲の整数として、変数qを： $q = z \# i$ の低位バイトとし、ここで、#はビットブール排他OR演算子とし、変数kを： $k = TBOX[q]$ とし、b(i)を： $b(i) = b(i) + k \bmod 256$ によってアップデートし、zを： $z = b(i) + z \bmod 256$ によって更新する。CMCの第2段階はインボリュートで、 $0 \leq i < (d-1)/2$ の範囲の全てのiに対して、 $b(i) = b(i) \# (b(d-1-i) \text{ OR } 1)$ によって処理し、ここでORはビットブール排他OR演算子である。CMCの最終段階は、第1段階に対して逆となる解読プロセスで：zの初期値を0とし、iを $0 \leq i < d$ の範囲の整数として、変数qを： $q = z \# i$ の低位バイトとし、変数kを： $k = TBOX[q]$ とし、zを： $z = b(i) + z \bmod 256$ によって更新し、b(i)を： $b(i) = b(i) - k \bmod 256$ によって更新する。図9に、選択された制御およびデータメッセージの暗号化および解読の、3段階のプロセスを示す。実施例では、第1段階および第3段階はそれぞれ、自動キー暗号化、解読プロセスである。自動キーシステムは、システムの出力がその後のシステム出力に影響するような、時間変化するシステムである。暗号化および自動キーシステムの詳細については、W.Diffie and M.E.Hellman, Privacy and Authentication: An Introduction to Cryptography, Proc. of the I.E.E.E., Vol.67, No.3, March 1979を参照のこと。

【0041】移動局ユニット装置

図10に移動局ユニットのハードウェアのブロック図を示す。制御ブロック200は、セルラ電話キーパッド、ハンドセット、ユニット電源制御スイッチ化ら構成される。制御ブロック200は、プロセッサ210へ接続され、音声信号のデジタル化、誤り訂正コードの組み入れ、デジタル音声信号の暗号化、入力音声信号の解読、種々の制御メッセージの形成および暗号化（解読）等を行うために、移動局ユニットの動作を制御する。ブロック210は、信号の送受信回路からなるブロック220へ結合される。ブロック200-220は基本的に従来方法のブロックで、現在市販の移動電話ユニット（市販のユニットでは暗号化および解読は行われたい）の機能を達成するものである。本発明の認証および暗号化プロセスのために、図8の装置にはさらに、多数のレジスタ

をプロセッサ210へ結合したブロック240が含まれ、“個別”モジュール230もプロセッサ210へ結合される。モジュール230は、移動電話ユニットの一部であるか、ソケットによって移動電話ユニットに着脱可能なモジュールであっても良い。モジュールは、電磁的にあるいは接続によってプロセッサ210へ接続される。モジュール230は例えば、“スマートカード”でも良い。

【0042】モジュール230は、ジャンブルプロセッサ231およびプロセッサ231の多数のレジスタから構成される。あるいは、他の実施例では、Aキーのみをモジュール230に配置しても良い。Aキー、MIN1およびMIN2呼称をブロック240のレジスタよりは、モジュール230のレジスタにインストール（および保持）する方が都合が良い。また、得られたSSDフィールドをモジュール230のレジスタに記憶させるのも好都合である。プロセッサ231の処理を実行するのに必要なレジスタを、モジュール230内に配置することが好ましい。モジュール230にこれらの要素を配置することによって、利用者はモジュールを持ち運んで異なった移動ユニットに用いることができ（例として、“拡張”移動ユニット）、より重要な情報の多くをモジュール以外に記憶させることができる。移動ユニットは、ユニットと一体化したモジュール230としても良い。そのような実施例では、ジャンブルプロセッサ231はプロセッサ210内に組み込まれる。ブロック240では、受信されるユニットのESN呼称および種々のRANDシーケンスを保持する。

【0043】本発明は、セルラ電話における加入者の認証に関するものであるが、ポータブルハンドセットを用いるパーソナル通信ネットワークも包含し、本発明の原理は、通信の安全性が十分に確保されない場合や、偽装者が問題となる場合にも有効である。例えば、コンピュータネットワークも含まれる。

【0043】

【発明の効果】以上に述べたように、本発明では、セルラ電話システムにおける暗号システムにおいて、可変長の元メッセージを、8ビットマイクロコンピュータによって簡単に暗号化および解読を行うことが可能な、比較的安全な、自己転換、対称キー暗号システムを提供することができる。

【図面の簡単な説明】

【図1】固定および移動電話の両方のサービスのために相互接続された、ネットワーク提供者およびセルラ無線提供者の構成を示す図である。

【図2】共有秘密データフィールドの作成と同一性の検証を行うプロセスを示す図である。

【図3】共有秘密データ作成のための各要素の接続および分割を示す図である。

【図4】検証シーケンス作成のための各要素の接続および分割を示す図である。

【図5】移動局ユニットの送信中の登録シーケンス作成のための各要素の接続および分割を示す図である。

【図6】呼び出しシーケンス作成のための各要素の接続および分割を示す図である。

【図7】移動局ユニットでの音声の暗号化および解読プロセスを示す図である。

【図8】再認証シーケンス作成のための各要素の接続および分割を示す図である。

【図9】選択された制御およびデータメッセージの暗号化および解読のための3段階のプロセスを示す図である。

【図10】移動局ユニットのハードウェアのブロック図である。

【符号の説明】

10-14 交換機

20-21 固定局

22-23 移動局

30-40 基地局

101 ジャンブルブロック

102 ブロック

104 ブロック

200 制御ブロック

210 プロセッサ

220 ブロック

230 モジュール

231 プロセッサ

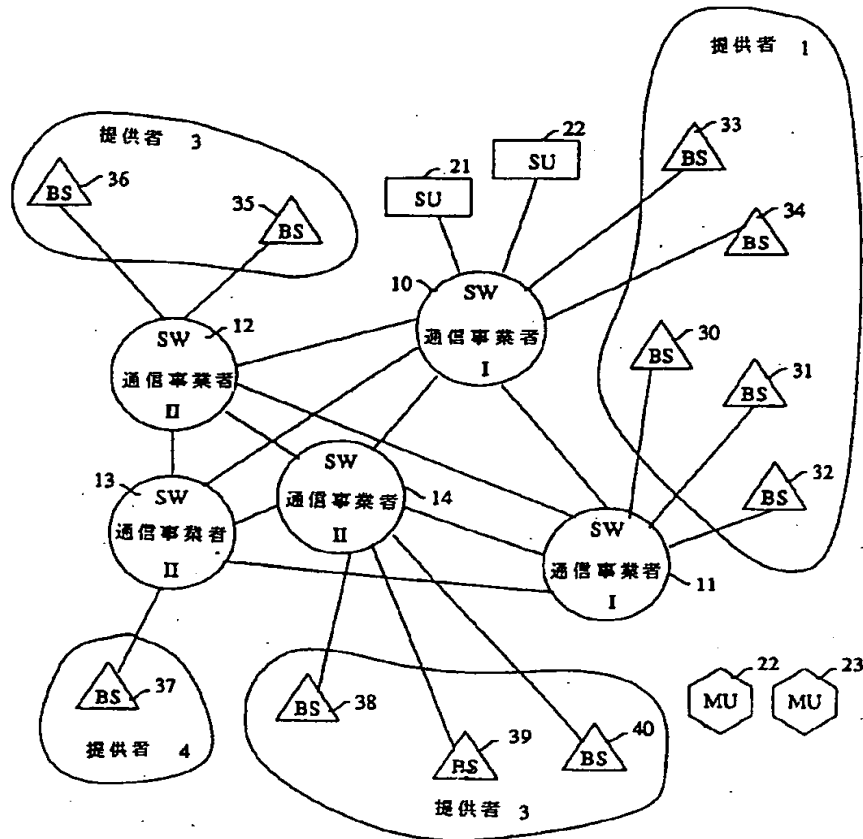
240 ブロック

301-303 要素

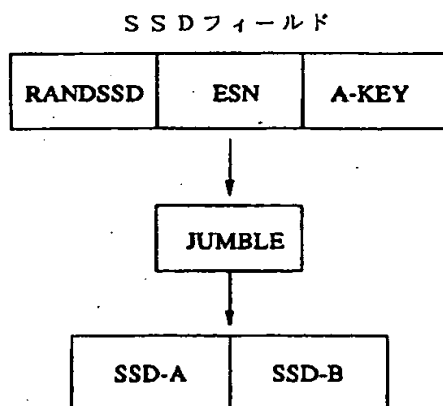
502 要素

504 要素

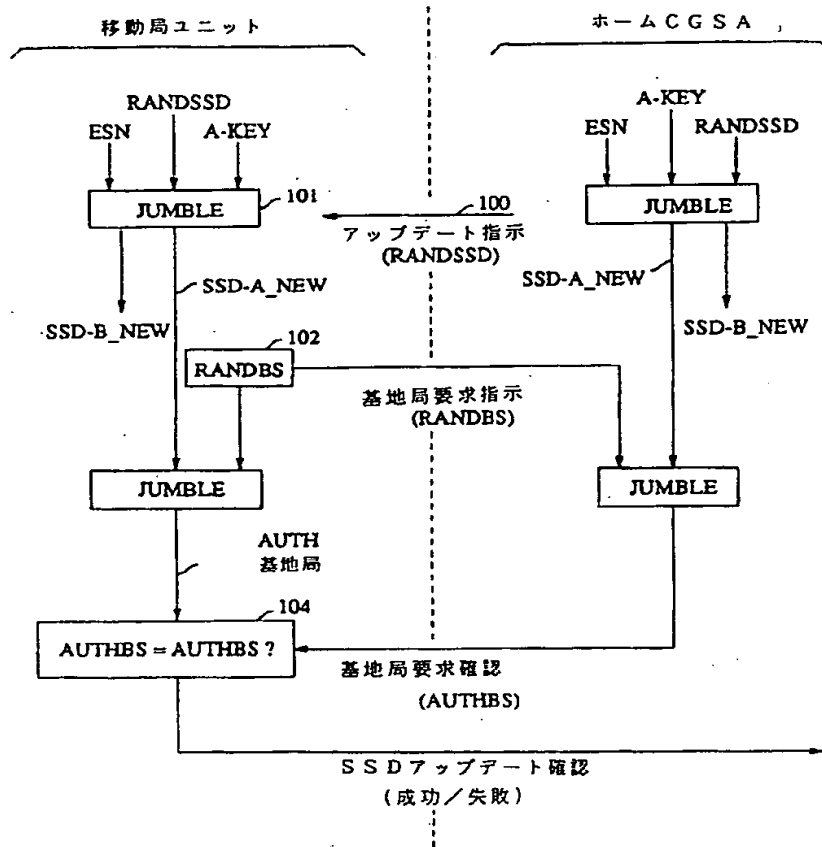
【図1】



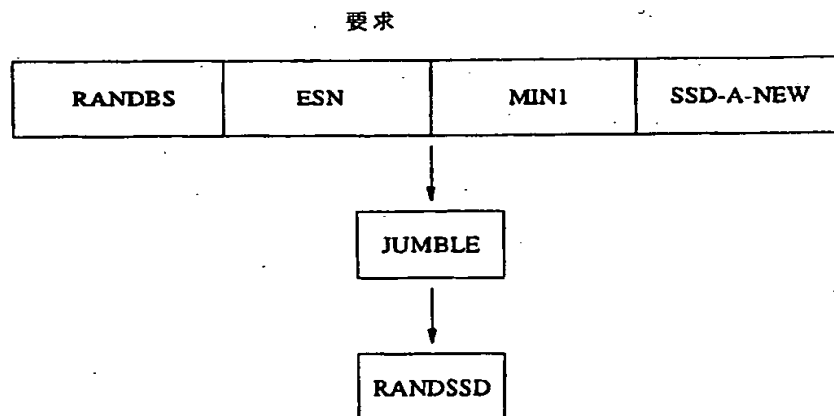
【図3】



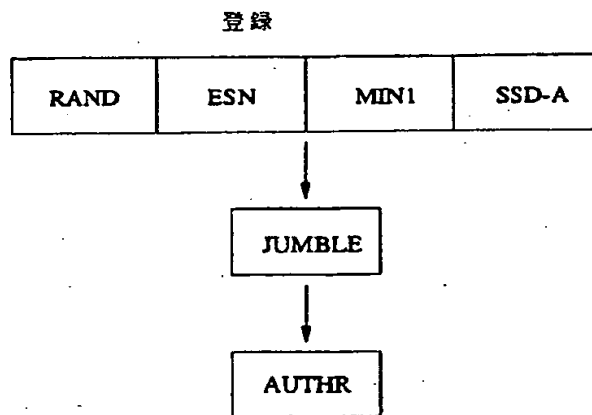
【図2】



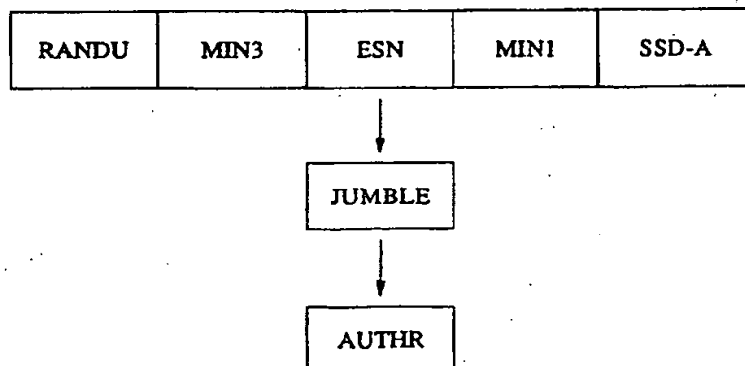
【図4】



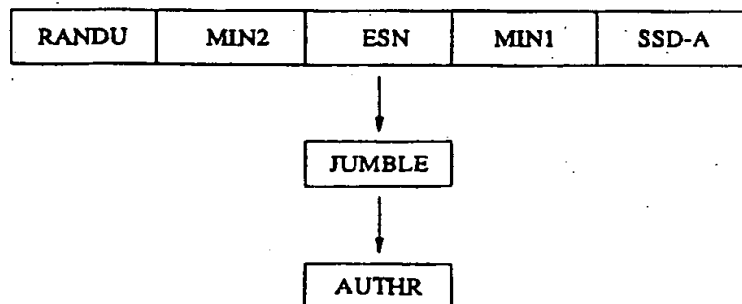
【図5】



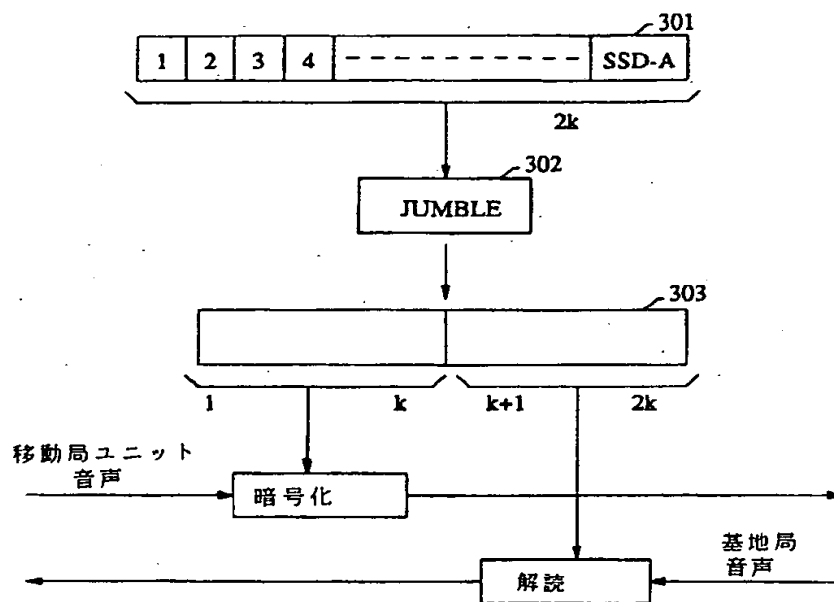
【図6】



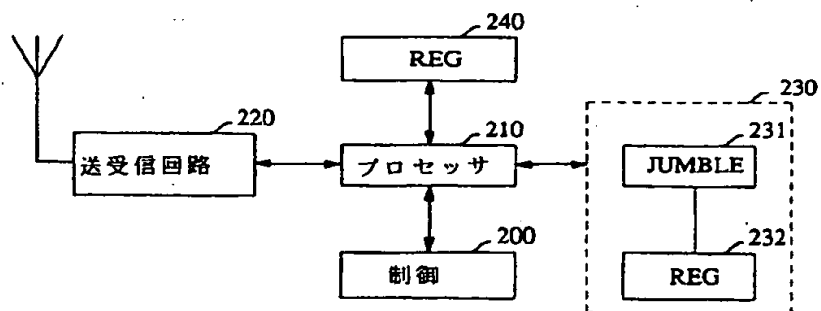
【図8】



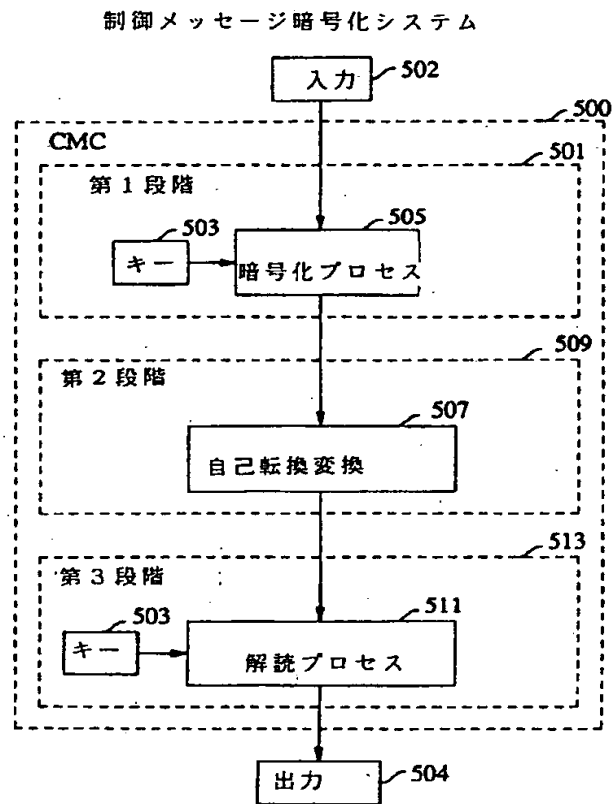
【図7】



【図10】



【図9】



フロントページの続き

(72)発明者 ジェームス アレクサンダー リーズ サード
 アメリカ合衆国 07974 ニュージャージー
 ニュー プロヴィデンス、サウスゲート
 ロード 127